(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09149022 A**

(43) Date of publication of application: **06.06.97**

(51) Int. Cl **H04L 9/12**
**G11B 20/10**
**// G06F 1/00**
**G06F 12/14**

(21) Application number: **07304122**

(22) Date of filing: **22.11.95**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

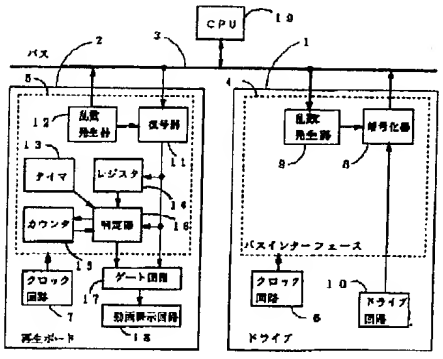
(72) Inventor: **OKABE YOSHIMASA**

(54) **DIGITAL DATA COMMUNICATION SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To protect a copyright by inhibiting illegal use of digital data from a disk in a personal computer(PC) system including a disk driver and a reproduction board connecting to a CPU bus.

SOLUTION: A drive 1 (reproduction board 2) is provided with a random number generator 9 (12) of the same system, a random number as an initial value is transferred from the reproduction board 2 to the drive 1, a random number resulting from ciphering only head data of a sector from the drive 1 is returned and a time required for return has a limit. Then sector data including the head data are transferred and a discrimination device 16 discriminates the coincidence with the head data to inhibit the use of illegal data thereby preventing copy of data with the copyright on the PC.



Title of the Prior Art

Japanese Published Patent Application No. Hei.9-149022

Date of Publication: June 6, 1997

[Claims]

[Claim 1] A digital data communication system wherein a first random number generator and a second random number generator for sequentially generating the same random number as each other after the respective initial values are set are positioned in a first unit and a second unit which are connected through a line, respectively, and prior to the transmission of digital data, the random number generated by the second random number generator is supplied to the first random number generator as an initial value through the line, and data of the head value of the sector data to be transmitted is encrypted on the basis of the random number generated by the first random number generator based on the initial value and the encrypted data is transmitted to the second unit, and subsequently the sector data inclusive of the head portion data of the sector data to be transmitted is encrypted on the basis of the random numbers which are sequentially generated by the first random number generator and the encrypted data is transmitted to the second unit, and the second unit decrypts the received encrypted head portion data on the basis of the random numbers which are sequentially

generated by the second random number generator and stores the decrypted data in a register, and subsequently decrypts the received encrypted sector data inclusive of the head portion data on the basis of the random number of the second random number generator, and judges whether or not the head portion data of the decrypted sector data matches the head portion data stored in the register, and when the number of mismatch times reaches a predetermined number of times, the communication between the first unit and the second unit is interrupted.

[Claim 2] The digital data communication system as defined in Claim 1, wherein

the second random number generator has no means for inputting an initial value, and an allowable limit of a difference between a time period required from transmitting a random number generated by the second random number generator to the first random number generator as an initial value through the line, to returning the encrypted data of the sector head portion data, which is encrypted on the basis of the random number generated based on the initial value, to the second unit from the first unit and a time period required for generation of the random number used for encrypting the sector head portion data, is set to half the time period required for generating the random number or less.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

**特開平9－149022**

(43)公開日　平成９年(1997)６月６日

| (51)Int.Cl.[6] | | 識別記号 | 庁内整理番号 | ＦＩ | | 技術表示箇所 |
|---|---|---|---|---|---|---|
| Ｈ０４Ｌ | 9/12 | | | Ｈ０４Ｌ | 9/00 | ６３１ |
| Ｇ１１Ｂ | 20/10 | | 7736－5D | Ｇ１１Ｂ | 20/10 | Ｈ |
| // Ｇ０６Ｆ | 1/00 | ３７０ | | Ｇ０６Ｆ | 1/00 | ３７０Ｅ |
| | 12/14 | ３２０ | | | 12/14 | ３２０Ｂ |

審査請求　未請求　請求項の数２　ＯＬ　（全６頁）

(21)出願番号　特願平7－304122

(22)出願日　平成７年(1995)11月22日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　岡部　吉正
香川県高松市古新町８番地の１　松下寿電子工業株式会社内

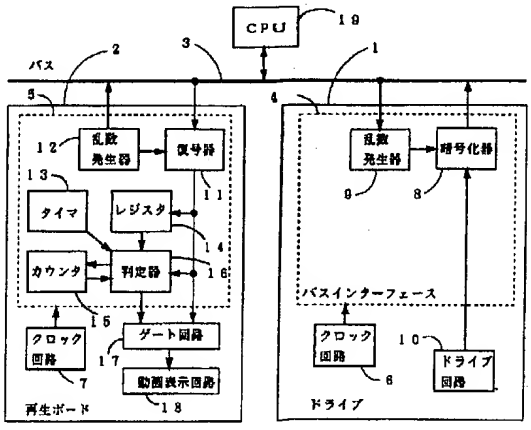
(74)代理人　弁理士　滝本　智之　（外１名）

(54)【発明の名称】　ディジタルデータ通信方式

(57)【要約】

【課題】　ＣＰＵバスに接続されるディスクドライブ装置と再生ボードを含むＰＣシステムにおいて、ディスクからのディジタルデータの不正使用を禁止し、著作権の保護を目的とする。

【解決手段】　ドライブ１と再生ボード２に同じ方式の乱数発生器９、１２を設け、再生ボード２から初期値としてドライブ１に乱数を転送し、ドライブ１からのセクターの先頭部データのみを暗号化した乱数を返送し、返送に要した時間に制限を設けると共に、次に前記先頭部データを含むセクターデータを転送し、先頭部データとの一致を判定器１６にて判定し、不正なデータの使用を禁止することにより、ＰＣ上での著作権のデータの複製使用を防止する。



1

【特許請求の範囲】

【請求項１】　回線を介して接続された第１の装置と第２の装置に、それぞれ初期値が定まるとその後は互いに同一の乱数を順次発生する第１の乱数発生装置と第２の乱数発生装置を配置し、ディジタルデータの送信に先立って、前記第２の乱数発生装置により発生された乱数を、前記回線を介して初期値として前記第１の乱数発生器に加え、その初期値に基づいて第１の乱数発生装置により発生された乱数により、送付すべきセクタデータの先頭値のデータを暗号化して前記第２の装置に送信し、続いてその送付すべきセクタデータの前記先頭部のデータを含むセクタデータを第１の乱数発生装置により順次発生される乱数により、暗号化して前記第２の装置に送信し、前記第２の装置においては、受信した前記の暗号化された先頭部のデータを前記第２の乱数発生装置により順次発生される乱数により復号化してレジスタに記憶し、続いて受信した前記先頭部のデータを含む暗号化されたセクタデータを前記第２の乱数発生装置の乱数により復号化し、その復号化されたセクタデータの先頭部データと前記のレジスタに記憶した先頭部データとの一致を判定し、不一致の回数が予め定められた回数に達すると第１の装置と第２の装置間の通信を遮断することを特徴とするディジタルデータ通信方式。

【請求項２】　第２の乱数発生装置が初期値を入力する手段を有せず、前記第２の乱数発生装置により発生された乱数を、前記回線を介して初期値として前記第１の乱数発生装置に送付してから、第１の装置から第２の装置に前記初期値を基に発生された乱数により暗号化されたセクタ先頭部データの暗号化データが返送されるまでに要した時間と、前記セクタ先頭部データの暗号化に用いる乱数の発生に要すべき時間との差の許容範囲を、前記乱数の発生に要すべき時間の半分以下に設定することを特徴とする請求項１記載のディジタルデータ通信方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディジタル通信サービスの不正利用の防止に有効なディジタルデータ通信方式に関するものであり、特に著作権の設定されたディジタルデータの複製防止に有効なものである。

【０００２】

【従来の技術】近年の記録技術の発達によって、小型の光ディスクに数ギガバイトのデータを記録することが可能になり、画像圧縮の技術によって、前記の光ディスクに映画をディジタル記録することが可能になった。他方ではパーソナルコンピューター（以後、ＰＣと略す）の発達と普及により、前記の光ディスクに記録された映画をＰＣのモニタ上に再生する利用法が出現した。この利用形態では、光ディスクを読み取るドライブ装置（以後、ドライブと略す）と、圧縮記録されている画像データを伸張して表示する再生ボードを、ＰＣのバスに接続し、このバスを経由して画像データの転送を行うことになる。

2

【０００３】ディジタルコピーは複製によって画質が劣化しないので、ＰＣのデータの複製や変造に適した機能を利用し、ＰＣ内のハードディスクドライブ（以後、ＨＤＤと略す）や磁気テープに画像データをコピーすることが可能であり、他のＰＣにもコピー可能である。しかし、映画ソフトには著作権が設定されていて複製や変造が禁止されているので、ＰＣが持つ複製機能が有効に機能しないようにすることが必要となる。

【０００４】ＰＣで映画を再生する場合、画像データはバスを通して伝送されるので、複製防止の問題はバス型伝送路における盗聴防止問題に帰結する。バス型伝送路では受動的な傍受を検知して防止することは困難なので、傍受したデータが利用できない様にデータを暗号化する暗号通信を行うのが一般的であり、暗号通信を行う為には、送信側と受信側は鍵とよばれる秘密の情報を共有する必要がある。

【０００５】秘密の情報を要求する点ではパスワードシステムとも呼ばれる暗証番号方式と暗号方式は同じである。特開平２－６７０６７号公報は、暗証番号を要求して、返答された暗証番号が不一致であるか、もしくは一定時間内に返答がない場合に接続を拒否する方式を提案している。特開平３－１０９８５０号公報は試行錯誤によって偶然に正しい暗証番号が入力される確率を小さくするために、入力開始から一定時間経過した時点で、正しい桁数の正しい暗証番号が入力されているかどうかを、１回だけ検査する方式を提案している。どちらの特許も、時間の設定方法には詳しい説明を加えてないが、平均的な利用者が暗証番号を入力するのに要する時間の最大値に設定すると考えるのが合理的である。

【０００６】図２は従来例のブロック図であり、２１はＣＰＵ、２２はバス、２３はドライブ、２４は再生ボード、２５はＨＤＤ、２６はバス監視ボードである。この従来例の動作は、ＣＰＵ２１がソフトウエアに従ってバス２２を介してドライブ２３と再生ボード２４に鍵の入力と更新を行い、ドライブ２３は鍵を用いてデータを暗号化して送出し、再生ボード２４は鍵を用いてデータを復元するものである。この方式は、データをＨＤＤ２５にコピーし、後でＨＤＤ２５から再生ボード２４にデータを転送しようとしても、鍵を発生するソフトウエアが前回と全く同じ動作をしない限り、暗号化時に用いられた鍵を再生ボード２４に入力できないので正常な再生を行うことができない。しかし、ユーザーがバス監視ボード２６をバスに接続し、バス監視ボード２６は再生ボード２４への鍵の書き込みを検知して鍵を取り込み、データをＨＤＤ２５に記録する際に、前記バス監視ボード２６の取り込んだ鍵も記録しておくと、後でＨＤＤ２５から再生ボード２４にデータを転送する際に、暗号化時に用いられた鍵を再生ボード２４に与えられるので正常な

再生ができる。

【０００７】

【発明が解決しようとする課題】このようにＰＣで著作権の有する画像及び音声データによる映画等を再生するシステムにおいては暗号鍵を秘密にしなければならない。ＰＣ利用者はディスク上の映画等が記録された画像及び音声データを複製する権利は持たないが、ディスクに納められた画像及び音声データより映画等を再生する正当な権利を持っている。

【０００８】ドライブと再生ボードは同じ鍵を共有する必要があるので、何らかの手段を用いてドライブと再生ボードに鍵を入力する必要がある。出荷時に予め同じ鍵を入力し、以後は変更しない方式では、ドライブが出力したデータを一旦、ＨＤＤにコピーし、ＨＤＤから再生ボードに入力した場合でも、再生ボードにはドライブから直接入力されたデータと区別する手段がないので、通常の再生と同様に映画が再生される。ＨＤＤからの再生が可能であれば、ＨＤＤ上のデータをコピーした他のＰＣでも再生が可能なので、固定の鍵を用いる方式はコピー防止として有効でない。

【０００９】映画の再生中に鍵を更新する方式を用いた場合でも、ドライブと再生ボードの間の鍵の交換はＰＣ内で行われるので、ＰＣ内のデータの流れを監視することで鍵の入手が可能である。

【００１０】従って、有効なコピー防止を施す為には単にデータを暗号化するだけでは十分でなく、再生ボードに入力されたデータが、ドライブから直前に出力されたデータと同一であることを再生ボードが確認できる通信方式が必要である。また、最悪のケースとして暗号と鍵に関する秘密がＰＣ利用者に暴露された場合でも、再生ボードを騙すことが極めて困難である方式が望ましい。

【００１１】本発明は上記従来の問題点を解決するもので、鍵の更新手順を模倣された場合でも、鍵の更新に要する時間を検査して通信を拒絶し、ディジテルデータの複製防止を実現するディジタルデータ通信方式を提供することを目的とする。

【００１２】

【課題を解決するための手段】前記課題を解決するために、本発明のディジタルデータ通信方式は、回線を介して接続された第１の装置と第２の装置に、それぞれ初期値が定まるとその後は互いに同一の乱数を順次発生する第１の乱数発生装置と第２の乱数発生装置を配置し、ディジタルデータの送信に先立って、前記第２の乱数発生装置により発生された乱数を、前記回線を介して初期値として前記第１の乱数発生器に加え、その初期値に基づいて第１の乱数発生装置により発生された乱数により、送付すべきセクタデータの先頭値のデータを暗号化して前記第２の装置に送信し、続いてその送付すべきセクタデータの前記先頭部のデータを含むセクタデータを第１の乱数発生装置により順次発生される乱数により、暗号化して前記第２の装置に送信し、前記第２の装置においては、受信した前記の暗号化された先頭部のデータを前記第２の乱数発生装置により順次発生される乱数により復号化してレジスタに記憶し、続いて受信した前記先頭部のデータを含む暗号化されたセクタデータを前記第２の乱数発生装置の乱数により復号化し、その復号化されたセクタデータの先頭部データと前記のレジスタに記憶した先頭部データとの一致を判定し、不一致の回数が予め定められた回数に達すると第１の装置と第２の装置間の通信を遮断することを特徴としたものである。

【００１３】本発明によれば、送信すべきデータの一部を用いてデータの正当性を判定するとともに、データの再生に必要な暗号鍵を不正に得ることが非常に難しく、複製防止に有効である。

【００１４】

【発明の実施の形態】本発明の請求項１に記載のディジタル通信方式は、回線を介して接続された第１の装置と第２の装置に、それぞれ初期値が定まるとその後は互いに同一の乱数を順次発生する第１の乱数発生装置と第２の乱数発生装置を配置し、ディジタルデータの送信に先立って、前記第２の乱数発生装置により発生された乱数を、前記回線を介して初期値として前記第１の乱数発生器に加え、その初期値に基づいて第１の乱数発生装置により発生された乱数により、送付すべきセクタデータの先頭値のデータを暗号化して前記第２の装置に送信し、続いてその送付すべきセクタデータの前記先頭部のデータを含むセクタデータを第１の乱数発生装置により順次発生される乱数により、暗号化して前記第２の装置に送信し、前記第２の装置においては、受信した前記の暗号化された先頭部のデータを前記第２の乱数発生装置により順次発生される乱数により復号化してレジスタに記憶し、続いて受信した前記先頭部のデータを含む暗号化されたセクタデータを前記第２の乱数発生装置の乱数により復号化し、その復号化されたセクタデータの先頭部データと前記のレジスタに記憶した先頭部データとの一致を判定し、不一致の回数が予め定められた回数に達すると第１の装置と第２の装置間の通信を遮断することを特徴としたものであり、データの正当性を判定するために使用するデータは、送信データの一部であり、かつセクタデータ毎に判定しているため、正当なデータの判定の信頼性を増すことができる。

【００１５】次に請求項２に記載されたディジタルデータ通信方式は、第２の乱数発生装置が初期値を入力する手段を有せず、前記第２の乱数発生装置により発生された乱数を、前記回線を介して初期値として前記第１の乱数発生装置に送付してから、第１の装置から第２の装置に前記初期値を基に発生された乱数により暗号化されたセクタ先頭部データの暗号化データが返送されるまでに要した時間と、乱数の発生に要すべき時間との差から得る許容範囲を、前記セクタ先頭部データの暗号化に用い

る乱数の発生に要すべき時間の半分以下に設定することを特徴としたものであり、不当な複製を行うには2／3倍以上の高速なクロック周波数で乱数を発生する乱数発生器を用意しないと正常にデータの復号ができず、また、第2の乱数発生器は初期値入力手段を持たないので、初期値を偽造されることがなく、安全な乱数発生器が得られ、信頼性の高いデータの再生が出来る。　以下に、本発明の請求項1、及び請求項2に記載された発明の実施の形態について、図1を用いて説明する。図1において、1はドライブ、2は再生ボード、3はバス、4、5はバスインターフェース、6、7はクロック回路、8は暗号化器、9、12は32ビット長さの乱数発生器、10はドライブ回路、11は復号器、13はタイマ、14はレジスタ、15はカウンタ、16は判定器、17はゲート回路、18は動画表示回路、19はCPUである。

【0016】以上の様に構成された映像再生システムの各部の動作を説明する。ドライブ1と再生ボード2はバス3に接続されている。バスインターフェース4、5はそれぞれクロック回路6、7が発生するクロックに同期して動作する。クロック回路6、7は同じ発振周波数で動作する。ドライブ側のバスインターフェース4は、暗号化器8と乱数発生器9とを持つ。暗号化器8は乱数発生器9が発生する乱数に従って、ドライブ回路10から入力されるデータを暗号化してバス3に出力する。乱数発生器9は、バス3を介して入力された32ビットの乱数を初期値として、初期値の入力後64クロック間は1クロック毎に1回、それ以外の期間は暗号化器8が読み出される毎に1回の割合で出力する乱数を順次更新する。

【0017】再生ボードのバスインターフェース5は、暗号化されたデータを復元する復号器11と乱数発生器12とタイマ13と、レジスタ14と、カウンタ15と判定器16を持つ。復号器11は乱数発生器12が発生する乱数に従って、バス3から書き込まれる暗号化データを元のデータに復元してレジスタ14と判定器16とゲート回路17に出力する。ゲート回路17は判定器16から禁止信号が出ていない期間は復号器11からの入力を動画表示回路18にそのまま出力するが、禁止信号が出ている期間はデータを出力しない。

【0018】ドライブ1から再生ボード2へのデータ転送はセクタと呼ばれる一定長のブロックを単位として行われる。前記乱数発生器12は、ドライブ1側の乱数発生器9と同一発生方式のものであり、両者の初期値が一致すると以後は両者とも同じ乱数を順次発生する。また、乱数発生器12は初期値を出力後、乱数発生器9と同期して、乱数の読出の64クロック後までの期間は1クロック毎に1回、それ以外の期間は復号器11にデータが書き込まれる毎に1回の割合いで乱数を更新する。但し、再生ボード2の乱数発生器12はドライブ1の乱数発生器9と異なり、乱数の初期値を入力する手段を持たないので、特定の初期値から乱数を発生する様に外部から制御することはできない。タイマ13は乱数発生器12が初期値を読み出してから、復号器11にドライブ1側より送られるセクタの先頭部のデータの暗号化されたデータが書き込まれるまでの時間を測定する。レジスタ14は復号器11が前記先頭部の暗号化されたデータ32ビットを復号した結果を記憶する。先頭部のデータのビット数は32ビットに限らず16ビット、8ビットでもPCのバス幅を考慮して決めればよい。



【0019】判定器16は乱数発生器12の乱数が読み出された時点からゲート回路17に禁止信号を出力する。タイマ13は乱数発生器12が乱数を送り出し、ドライブ1側から先頭部のデータが返ってくるまでの時間を計測し、タイムオーバを監視し、カウンタ15はタイマ13のタイムオーバーと先頭部のデータの値の不一致時カウントアップし、カウンタ値が8未満の場合は、復号器11が先頭部のデータを出力した時点の次のクロックでゲート回路17への禁止信号の出力を停止するが、カウンタ15の値が8の場合は、そのまま禁止信号の出力を続ける。乱数発生器の読み出し後の先頭の復号データはカウンタ15の値によらず動画表示回路18には出力されず、即ち、セクターの先頭部のデータはセクタの転送の度に一度データチェック用に用いられる。判定器16は復号器11から2番目のデータが出力された時点で、復号器11の出力とレジスタ14の出力が、セクターの先頭部のデータが一致し、かつ、タイマ13の値が80以下である場合にはカウンタ15を0にクリアするが、そうでない場合であってカウンタ15の値が8未満の場合は値を1だけ増やす。この時点の次のクロックでタイマ13は0にクリアされる。

【0020】即ち、タイマ13はクロックの数をカウントし、セクターの先頭部のデータの転送に先立って、64クロックカウント後、前記セクターの先頭のデータの暗号化データを受け取るまで計数し、計数値が80を越えるとタイムオーバーとしてカウンタ15をカウントアップする。

【0021】次に、1セクタのデータをドライブ1から再生ボード2に転送する場合の動作を、時間の流れに従って順に説明する。データ転送にはCPU19が介在する。まず、ドライブ回路10のバッファメモリに1セクタのデータが読み出し済みであり、動画表示回路18のバッファメモリに1セクタのデータを受け入れる空き容量があるとCPU19が判断した時点でデータ転送の手順が始まる。CPU19は乱数発生器12から乱数を読み出して乱数発生器9に乱数の初期値として入力する。乱数発生器12からの乱数の読み出しでタイマ13のカウントアップを開始し、乱数発生器12はこの時点から64クロック連続の乱数更新を行う。

【0022】乱数発生器9は初期値が入力されると64

クロック連続の乱数更新を行い、暗号化器８に出力する。暗号化器８にはドライブ回路１０からのセクターの先頭のデータが出力されているので、暗号化器８の出力は１セクタの予め定められたビット数の先頭のデータを暗号化した結果になる。ＣＰＵ１９は乱数の更新が終了するのを待って暗号化器８の出力を読み出し、この暗号化された先頭のデータを復号器１１に書き込む。この時の読み出しは本来のデータ転送ではないので、ドライブ回路１０のバッファメモリの状態は変化しない。

【００２３】復号器１１に暗号化データが書き込まれた時点でタイマ１３のカウントアップが停止する。ＣＰＵ１９が再生ボード２からドライブ１へ乱数を、ドライブ１から再生ボード２へ暗号化データを転送する合間に余分な動作をしていなければタイマ１３の値は６４より余り大きな値にはなっていないはずである。また、この時点で乱数発生器９と乱数発生器１２は同じ初期状態から同じステップ数だけ状態遷移を繰り返したので同じ乱数を出力しているはずである。従って復号器１１は乱数発生器１２の出力に従って、暗号化器８が乱数発生器９の出力に従って行った操作と逆の操作を行い、その結果として１セクタの先頭のデータを出力する。但しこのデータは本来のデータ転送ではないので動画表示回路１８には出力せず、レジスタ１４にだけ記憶する。

【００２４】次に、前記先頭のデータを含む１セクタ分のデータの転送を開始する。セクタのデータは乱数発生器９が発生した新たな乱数に従って暗号化器８により暗号化され、ＣＰＵ１９によって復号器１１に転送されて、乱数発生器１２の出力に従って復元される。判定器１６はセクタの先頭のデータとレジスタ１４の出力を照合し、一致しなければデータの送り側が真正なドライブでないと判断してカウンタ１５をカウントアップし、一致した場合であってもタイマ１３の値が８０以上の場合もタイムオーバーとして、送り側の乱数発生器が模造品であると判断してカウンタ１５をカウントアップする。カウンタ１５の値が８になるとゲート回路がデータを出力しなくなるので、再生はストップする。もちろん、再生をストップさせるカウンタの値は８以外の整数値を選定してもよい。

【００２５】最後に、本発明を適用する場合の要点を説明する。まず、受信側から送信側へ乱数を送り、送信側から受信側へと暗号化データを送るのに要する最短時間を求め、これと送信側において入力された乱数（送信側での乱数発生器９の初期値となる）から返送に用いる乱数の発生に要すべき時間との差の許容範囲を、乱数の発生に要すべき時間の半分以下になるように乱数の連続更新の回数を設定し、判定器が許容する遅延時間のクロック数を連続更新のクロック数の１．５倍以下に設定する。

【００２６】不正に複製したデータを再生しようと試みるものが、乱数発生器と暗号化器を市販のＩＣを組み合



わせて構成しようとした場合、自作の回路を専用ＩＣと同じクロック周波数で動作させるのは極めて困難であるが、半分以下の低いクロック周波数で動作させることは比較的容易である。また、応答時間の制限が緩ければ、乱数の計算をソフトウエアで実行することも可能である。このように、応答の制限時間を不必要に大きくすると不正利用が容易になる。本発明では乱数の返送に要する時間を、専用の乱数発生器が乱数の生成に要する時間の１．５倍以下に厳しく制限することにより、ソフトウエアや自作の乱数発生器などによって受信側が騙されることを防止している。

【００２７】ＰＣシステムのバスは必ずしも一体物ではなく、ブリッジを介して異なる速度で動作するバスが中継され、インターフェースを介して各種の装置間のデータ転送が行なわれる複雑な伝送路である。伝送路としての遅延要因には、ブリッジやインターフェースといった静的な遅延要因の他に、割り込みやメモリリフレッシュといった動的に変化する遅延要因があり、真正の装置間でも必ずしも前記の最短時間内に応答が返るとは限らない。しかし、遅延時間のばらつきを考慮して時間制限を緩めると不正利用に対して弱くなる。本発明では、動的要因による時間切れやデータの伝送誤りに対しては通信の中断が起きないように、応答が正しくないかタイムオーバである場合にはカウンタをカウントアップし、カウンタが上限に達した時点で通信を中断する方式を用いる。動的要因によって大きな遅延が生じる確率が十分に小さく、カウンタの上限値が十分に大きければ、動的要因によって通信が中断する確率は実用的な観点から見てゼロと見なせる。一方、自作の乱数発生手段の動作速度の制限による遅延時間は静的な遅延要因なので、時間切れが毎回発生してカウンタは短時間で上限値に達し、確実に通信の中断が発生する。受信側の乱数発生器に初期値を入力できないことは重要である。もし、初期値の入力が可能であれば、送信側に送る乱数が特定の値になるように制御することが可能になる。特定の初期値入力に対する応答は別の特定の値になるので、前記の別の特定の値を応答するプログラムを作成して、受信側を騙して不正に複製したデータを処理させることは容易である。受信側の乱数発生器には初期値の入力手段を設けるべきではなく、もし設ける場合には十分な隠蔽を施すべきである。

【００２８】

【発明の効果】以上のように、本発明のディジタルデータ通信方式によれば、乱数の発生時間の制限とセクターの先頭データの一致をセクターの転送毎に判定することにより、本来の装置から別の装置にコピーされたデータの処理を拒否することが可能であり、特に、暗号に関する秘密が破られた場合にも、乱数発生時間の制限からデータの不正利用を極めて困難にすることができる。

【図面の簡単な説明】

9　　10

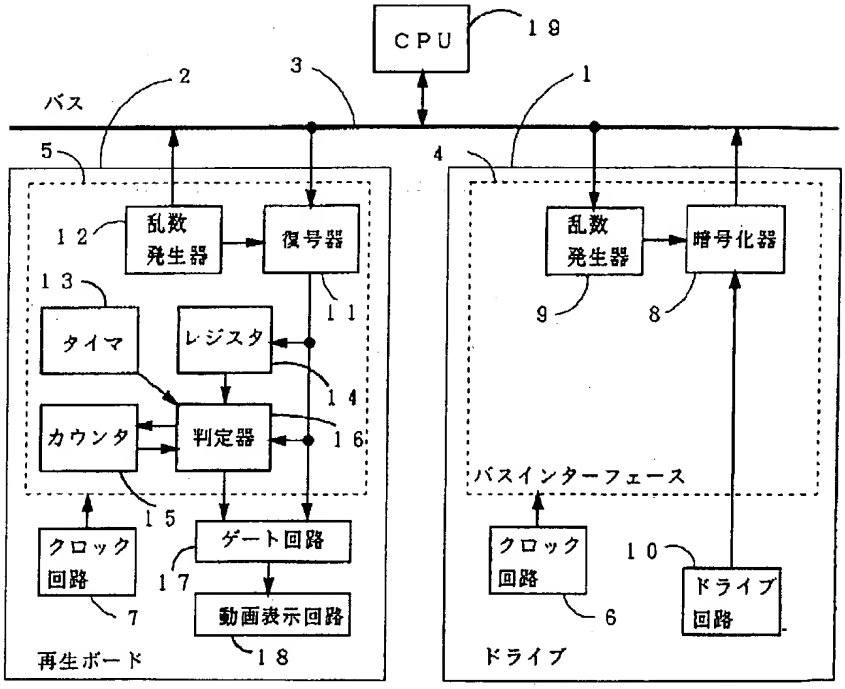
【図１】本発明の実施の形態におけるディジタルデータ通信方式を示すブロック構成図

【図２】従来例のデータ通信方式におけるブロック構成図

【符号の説明】

１、２３　ドライブ
２、２４　再生ボード
３、２２　バス
４、５　バスインターフェース
６、７　クロック回路
８　暗号化器
９、１２　乱数発生器
＊１０　ドライブ回路
１１　復号器
１３　タイマ
１４　レジスタ
１５　カウンタ
１６　判定器
１７　ゲート回路
１８　動画表示回路
１９、２１　ＣＰＵ
２５　ＨＤＤ
２６　バス監視ボード

【図１】




【図２】